VPN Configuration of NETGEAR DG834/DG834G-to-FVL328

This is a case study on how to configure a secure IPSec VPN tunnel between a NETGEAR DG834/DG834G and a NETGEAR FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Configuration Overview

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

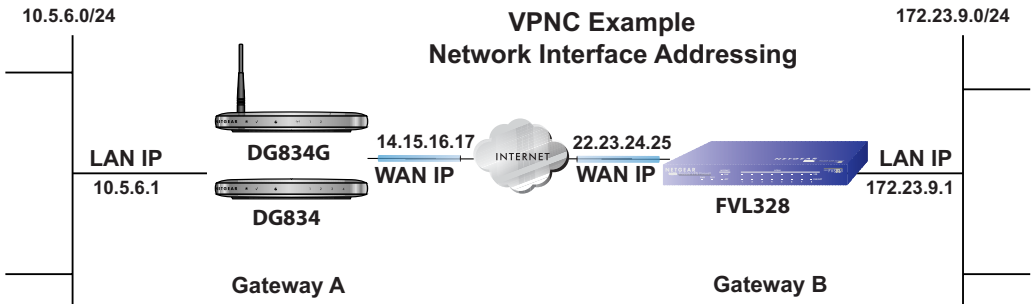

Figure 1: Addressing and Subnets Used for Examples

	Note: Product updates are available on the NETGEAR, Inc. web site at *http://www.netgear.com/support/main.asp*.

DG834/DG834G Scenario 1: DG834/DG834G to Gateway B IKE and VPN Policies

Table 1-1. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		April 2005
Model/Firmware Tested:		
	NETGEAR-Gateway A	DG834/DG834G firmware version V2.10.17
	NETGEAR-Gateway B	FVL328 with firmware version V2.0_07
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying

- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

Configuring the VPN Tunnel

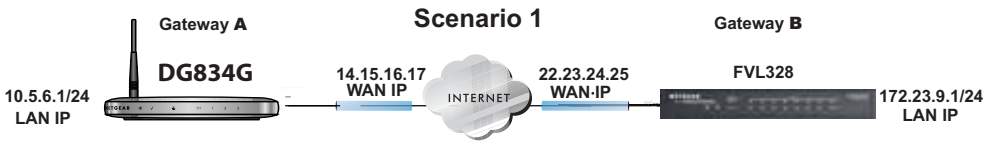

Figure 2: LAN to LAN VPN access from a DG834/DG834G to an FVL328

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the DG834/DG834G labeled Gateway A as in the illustration.**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

2. **Use the VPN Wizard to configure the DG834/DG834G at Gateway A.**

   Follow the steps listed in Figure 3 and Figure 4 using the following parameters:

   - Connection Name: **Scenario_1** (in this example)
   - Pre-Shared Key: **hr5xb84l6aa9r6**
   - Remote WAN IP address: **22.23.24.25** (in this example)
   - Remote LAN IP Subnet
     - IP Address: **172.23.9.1** (in this example)
     - Subnet Mask: **255.255.255.0** (in this example)

	Note: The LAN IP subnet at one end of the VPN tunnel must be different from the LAN IP subnet at the other end of the VPN tunnel. For example, if one side's LAN subnet is 192.168.0.x, then the other side should be 192.168.1.x (the subnet mask in this example is 255.255.255.0).

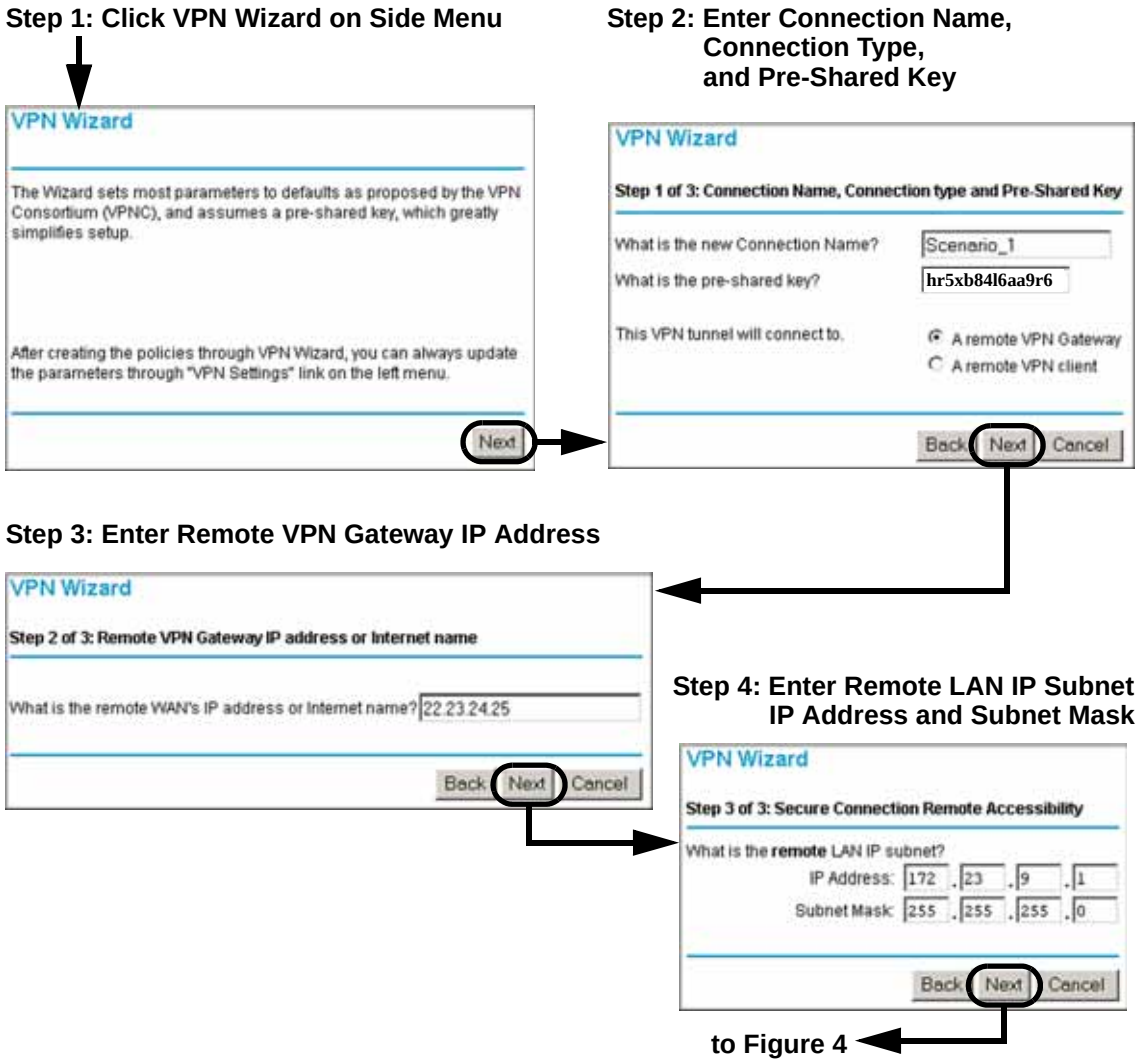

Figure 3: Netgear's VPN Wizard for the DG834/DG834G at Gateway A (part 1 of 2)

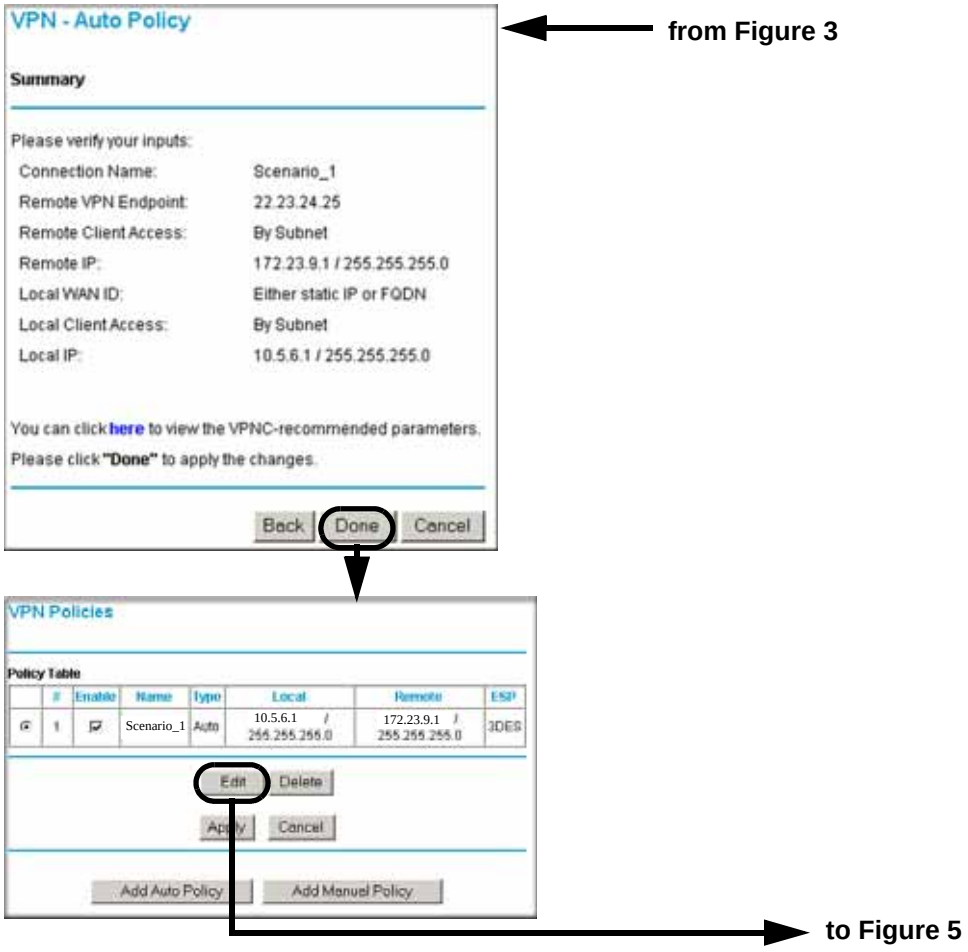

Figure 4: Netgear's VPN Wizard for the DG834/DG834G at Gateway A (part 2 of 2)

3. **Edit the policy just created in the VPN Policies window (see Figure 5).**
   a. Change the **SA Life Time** to **28800** seconds.
   b. Check the **Enable PFS** option.
   c. Click **Apply**.

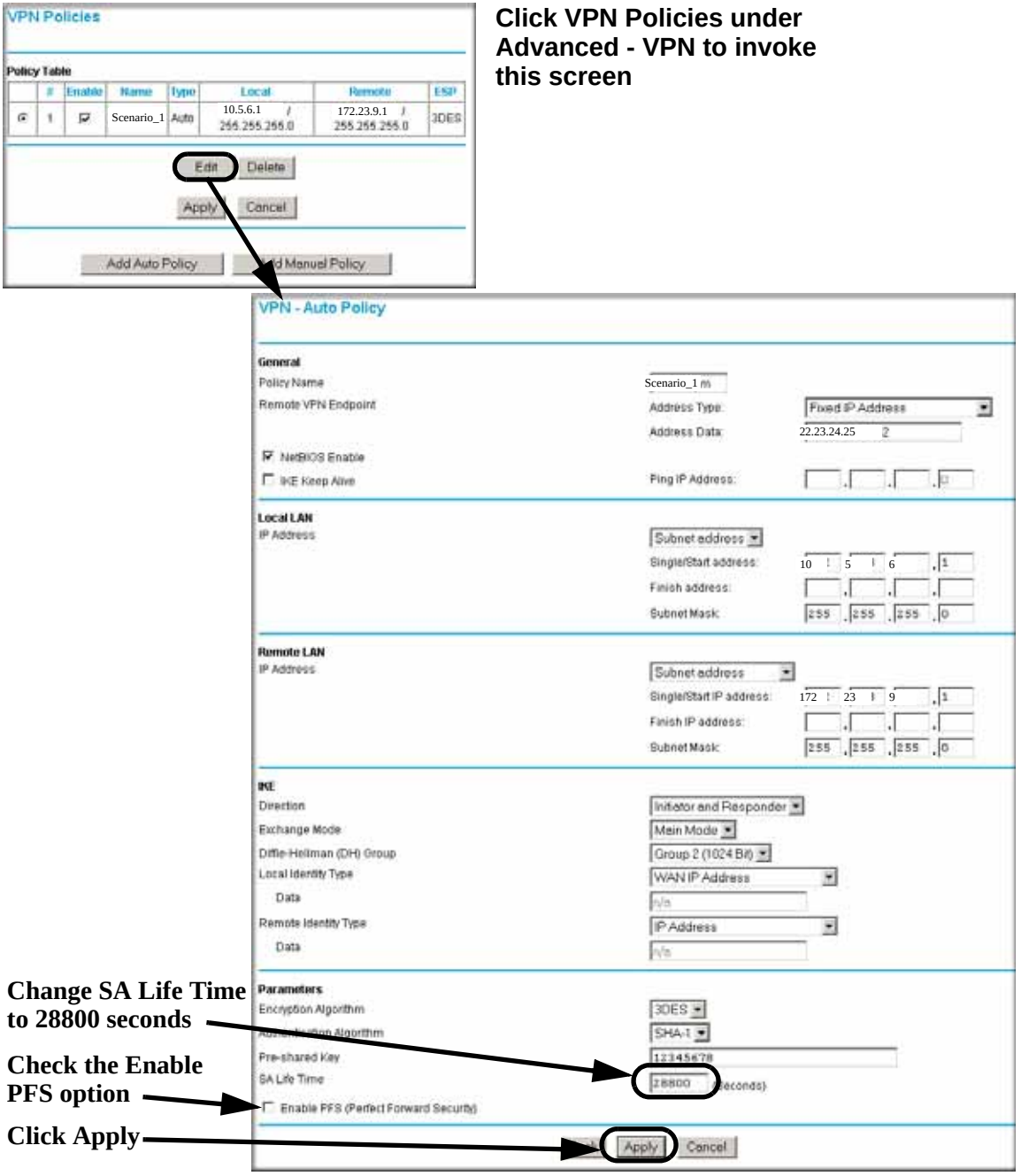

Figure 5: Viewing and Editing the VPN Parameters of the DG834/DG834G at Gateway A

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the DG834/DG834G according to the following testing flowchart:

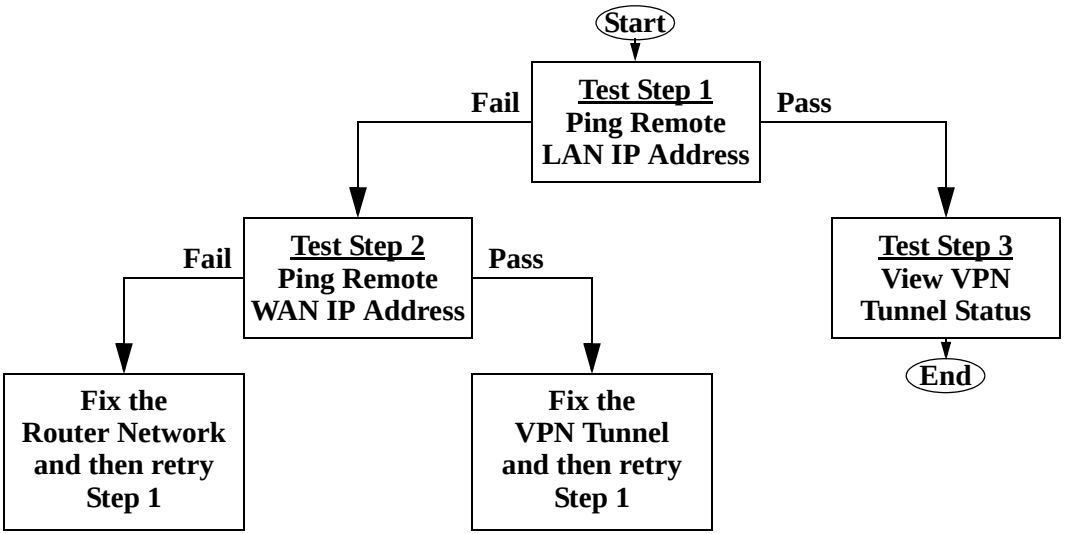

Figure 6: Testing Flowchart

To test the Gateway A to B VPN tunnel, do the following:

1. **Ping Remote LAN IP Address**: To establish the VPN connection between the DG834/DG834G Gateway A and Gateway B tunnel end points, perform these steps:

   a. Using our example, from a PC attached to the DG834/DG834G on LAN A, on a Windows PC click the **Start** button on the taskbar and then click **Run**.

   b. Type **ping -t 172.23.9.1**, and then click **OK**.

      This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.

2. **Ping Remote WAN IP Address**: To test connectivity between the DG834/DG834G Gateway A and Gateway B WAN ports, follow these steps:

   a. Enable “Respond to Ping on Internet Port” for the FVL328 in the WAN Setup menu under Advanced.

b. Using our example, from a PC attached to the DG834/DG834G on LAN A, on a Windows PC click the **Start** button on the taskbar and then click **Run**.

c. Type **ping 22.23.24.25**, and then click **OK**.

This causes a ping to be sent to the WAN interface of Gateway B. If there is no response, there is a network problem which must be resolved. Check that the gateway at each side of the tunnel has Internet access and that the addresses are correct. When the WAN ping works, try step 1 again.

3. **View VPN Tunnel Status**: To view the DG834/DG834G event log and status of Security Associations, follow these steps:

a. Go to the DG834/DG834G main menu VPN section and click the **VPN Status** link.

b. The VPN Status/Log screen displays a history of the VPN connections and the Current VPN Tunnels (SAs) table reports the status and data transmission statistics of the VPN tunnels for each policy.

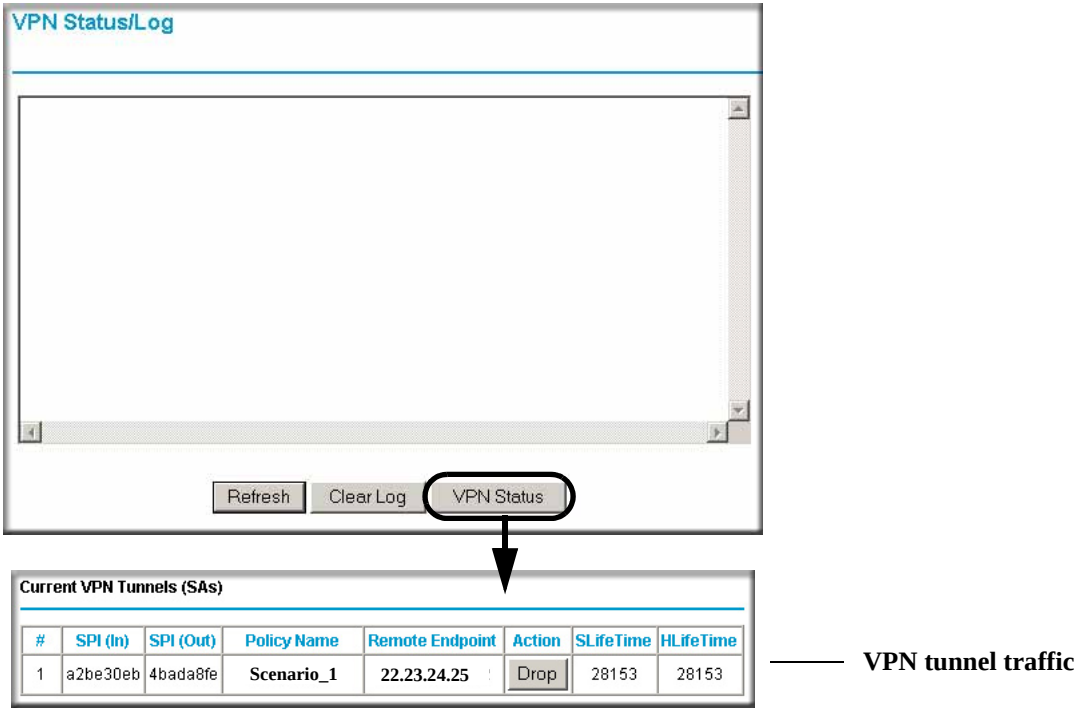

Figure 7: VPN Status/Log for the DG834/DG834G at Gateway A